

**REMARKS/ARGUMENTS**

Claims 1-10 and 16-20 now stand in the resent application, claims 1, 2, 4, 5, 7 and 9 having been amended and new claims 16-20 having been added.

Reconsideration and favorable action is respectfully requested in view of the above amendments and the following remarks.

In the Office Action, the Examiner has indicated that the amendment of the specification submitted in the Amendment dated May 5, 2008 is not entered at this stage of the prosecution. However, the Examiner gives no reason as to why this amendment to the specification has not been entered. The Examiner does not claim that the amendment constitutes new matter and in fact the Examiner's argument seems to be with respect to what one of the cited references, namely, Farber discloses. This has nothing to do with whether or not Applicants' amendment to the specification is entitled to be entered or whether it should not be entered because it constitutes new matter. Accordingly, Applicants request the Examiner to reconsider his decision and to enter the specification amendment as set forth in the previous May 2, 2008 Amendment.

The Examiner has also rejected claims 1-10 under 35 U.S.C. § 103(a) as being unpatentable over Farber et al. ("Farber") in view of Brickell. As noted above, Applicants have amended the present claims in order to more clearly patentably define over the cited art as will be explained in greater detail below.

Farber nowhere in its disclosure mentions digital signatures. Applicant's claims 1-6, 8, 10, 16-18 and 20 require that the digital signature is created using a signing key.

Farber nowhere in its disclosure mentions signing keys. The Examiner indicates that Farber teaches the use of a 'message digest code (MAC)'. While Farber does teach the use of 'message digests' to check the integrity of a file, it does **not** teach the use of MAC's or Message Authentication Codes – which are created using a signing key. In fact, Farber does not once mention authentication.

The Examiner appears to accept that Applicant's claims are novel over Farber since they include digital signatures.

Brickell states that digital signatures provide both integrity-checking (a function performed using hash functions in Farber) and authentication ('... and to enable the verification of the identity of the transmitting party' – see Brickell at col. 1, lines 52-53 – i.e., to authenticate the transmitting party).

The Examiner's argument is that a person skilled in the art would read and understand Farber, see that it lacked an authentication mechanism, and therefore introduce the digital signatures seen in Brickell. However, even if, *arguendo*, skilled persons were to do that, they would not arrive at a system which falls within Applicant's claims. That is because the skilled person would first have to determine who is to sign the file. There are no clear directions in Farber as to who might sign the file (Farber nowhere contemplates signatures or authentication). Brickell, unsurprisingly, teaches the skilled person that a message should be signed by "the party sending the transmission." See Brickell at col. 1, lines 47 and 48.

Transmitting a file in Farber appears to involve a local processor executing its 'Realize True File From Location' primitive (Farber at col. 16, lines 10 to 37) which uses the 'Request True File' service (Farber at col. 24, lines 45 to 62) offered by the remote processor which has the file. Applying the teaching of Brickell to Farber would mean that some process at the remote processor would sign the file. Since Farber carries out its integrity check on receipt at the local processor (Farber at col. 16, line 36), it follows that a skilled person would check the signature on the file on receipt at the local processor. This is also what Brickell teaches the skilled person to do – to carry out its signature check (i.e., authenticity check) on receipt of the message (Brickell at col. 6, lines 45 to 47). Hence, even if skilled persons were to modify Farber in view of Brickell, they would not arrive at a server computer including a:

means arranged to deny said other computer access to said at least one requested computer file if the digital signature or signatures associated with each respective requested computer file is invalid.

See, for example, amended claim 1 (emphasis supplied). There is no suggestion in Farber or Brickell that an authenticity check should be made by the sender of a file or message. This feature of a server-side authenticity check is counter-intuitive. Applicant's introduction of an authentication check at a server computer is non-obvious, and Applicant's claims in this regard patentably define over the cited art taken singly or in combination.

Indeed, the Examiner's rejection of independent claims 1, 4, 5, 7, and 9 and their respective dependent claims is flawed. The only passage amongst the many in Farber cited by the Examiner which is of any relevance to the question as to where an integrity

check is carried out is the passage at col. 34, lines 33 to 50. When looked at in the best possible light to sustain the rejections and applying a good deal of informed speculation to what is meant in that passage, the passage perhaps discloses a mechanism for protecting the system against viruses. Infecting an executable file with a virus involves modifying the executable file. Hence, if an administrator wants to provide each processor in the system with a suite of Microsoft Office applications, then the administrator would create a region ... usr/bin/office on each processor – that region including executable files word.exe, etc. Farber contemplates that the system would store the True Names of 'clean' – i.e., not infected by a virus – copies of the Office applications somewhere (col. 34, lines 38 and 39). Farber then suggests that the 'Verify Region' mechanism might be used to check that the applications in the region hash to the True Name stored somewhere in the system for the application.

Once again, in Farber, the integrity check is carried out at the processor receiving the files and not at the processor providing the files, as required in the present claims. Furthermore, in relation to this sort of virus checking, there is no need for authentication, either the file is a clean copy of, for example, word.exe, or it isn't. The addition of an authentication check in that instance would be nugatory, and the skilled person would not make such an addition. Hence, even if skilled persons were to modify this aspect of Farber in view of Brickell, they would not arrive at a system including a:

means arranged to deny said other computer access to said at least one requested computer file if the digital signature or signatures associated with each respective requested computer file is invalid.

See, for example, amended claim 1 (emphasis supplied).

There is simply no suggestion in col. 34, lines 33 to 50 of Farber (or any of the other passages from Farber which the Examiner cites) that an authenticity check should be made by the sender of a file or message. Nor is this limitation taught or suggested by Brickell. This feature of a server-side authenticity check is counter-intuitive. Applicant's introduction of an authentication check at a server computer is non-obvious, and Applicant's claims in this regard patentably define over the cited art taken singly or in combination.

With respect to present claim 2, it is respectfully submitted that the Examiner's reference to Brickell at col. 7, lines 45-47 does not disclose "a store arranged to store a list of approved computer file signing parties." More generally, digital signature protocols often involve 'trusted third parties' also known as 'certification authorities' who certify that a public key belongs to a given organization or individual. They certify that fact by themselves signing the organization or individual's public key with the certification authority's private key. It is the certification authority's signature which is being discussed at col. 7, lines 45-47 of Brickell, not the signature of the sender of the message. Importantly, what is being signed in Brickell at col. 7, lines 45-47 is a digital certificate, not a file stored on the server computer.

Accordingly, for all of the above reasons, it is respectfully submitted that the present claims patentably define over the cited art taken singly or in combination.

Therefore, in view of the above amendments and remarks, it is respectfully requested that the application be reconsidered and that all of claims 1-10 and 16-20, now standing in the application, be allowed and that the case be passed to issue. If

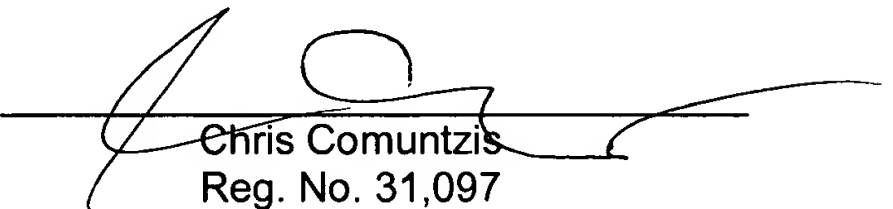
WRIGHT, et al.  
Appl. No. 09/936,210  
January 30, 2009

there are any other issues remaining which the Examiner believes could be resolved through either a supplemental response or an Examiner's amendment, the Examiner is respectfully requested to contact the undersigned at the local telephone exchange indicated below.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By:

  
Chris Comuntzis  
Reg. No. 31,097

CC:lmr  
901 North Glebe Road, 11th Floor  
Arlington, VA 22203-1808  
Telephone: (703) 816-4000  
Facsimile: (703) 816-4100